

ABSTRACT

A method and apparatus for performing modular multiplication is disclosed. An apparatus in accordance with one embodiment of the present invention includes a modular multiplier including a plurality of independent computation channels, where the plurality of independent computation channels includes a first computation channel and a second computation channel, and a coupling device interposed between the first computation channel and the second computation channel to receive a control signal and to couple the first computation channel to the second computation channel in response to a receipt of the control signal.